DEUSOP07 – Analysis, Interpretation and Reporting of Results

Table of Contents

1. Scope

1.1. The standard operating procedure is utilized for the analysis and reporting of digital evidence.

2. Background

2.1. To establish the practices for documenting the examination of evidence to conform to the requirements of the Department of Forensic Sciences (DFS) Forensic Science Laboratory (FSL) *Quality Assurance Manual*, the accreditation standards under ISO/IEC 17025:2005, and any supplemental standards.

3. Safety

3.1. Not applicable

4. Materials Required

4.1. Forensic examination workstation; forensic software; DEU media; DEU Forms; Case file(s)

5. Standards and Controls

5.1. Not applicable

6. Calibration

6.1. Not applicable

7. Procedures

7.1. Digital Evidence Analysis

7.2. This is a general procedure for analysis conducted by the digital evidence unit. For reporting and procedural purposes, analysis is not an extraction of data that is covered by acquisition SOPs. Analysis is an examination of the data once extraction per the scope/requirements of the request.

7.2.1. Determine and document a Scope of Examination with the requester. Use the warrant provided, if applicable and the request form submitted. This can be documented on DEUF05 Forensic Examination Form.

7.2.2. Ensure that the forensic workstation is up to date with DEU current software and hardware. Ensure no other examination is being undertaken.

7.2.3. Based on the scope of the analysis, determine what forensic tools are to be used. Record these items using DEUF05-Forensic Examination form. A basic analysis should include the following:

7.2.4. Add the working copy to forensic software.

7.2.5. If applicable to the image being analyzed, ensure that a verification hash is established prior to the commencement of the examination on the working copy. Log and record this as part of the case file. This can be documented via a DEU form, screen shot or other accessible documented method.

7.2.6. If possible and applicable, ensure that any folders/files are recovered from the working copy image.

7.2.7. If possible and applicable, utilize the NSRL hash libraries to perform a hash value and file signature analysis.

7.2.8. If possible and applicable, run the appropriate processing functions for type of image (Windows, Mac, Linux/Unix, Android, iOs, etc.) for unique system software/hardware identifiers.

7.2.9. Based on the scope and pre-determined tools, record methodology, tools and actions taken to retrieve pertinent data from working copy. This is recorded on DEUF05-Forensic Examination Form.

7.2.10. During the examination, document any third party or internally generated functions, scripts ran or code that was used to analyze the data. This is recorded on DEUF05-Forensic Examination Form.

7.2.11. If practical, extract/export any relevant data for later inclusion in the forensic report.

DEUSOP07 – Analysis, Interpretation and Reporting of Results   Page **2** of **5**
Document Control Number: 2883   Approved By: Director
Revision: 2   Issue Date: 7/27/2018 6:04:06 PM
UNCONTROLLED WHEN PRINTED

7.2.12.   If tools used are not validated or validated by a standards body (NIST), the results must be verified using a secondary forensic tool and/or manually recalculated.

7.2.13.   At the completion of the analysis, produce a verification hash of the digital working copy, if applicable. Record the action on the DEUF05-Forensic Examination Form or note results in electronic case file (e.g., log file).

7.2.14.   Document a conclusion / finding based on the results of analysis and include references to the data used in determining the finding. Record items on the DEUF05-Forensic Examination form for inclusion in report.

7.2.15.   Follow steps in 7.2 to produce a report.

7.2.16.   In LIMS mark "Draft Completed" for technical and administrative review.

7.2.17.   Inform the technical leader or designee that the request is ready for technical and administrative reviews.

7.3.   DEU Reporting

7.4.   There are three types of reports and analysis that the DEU provides to requesting agencies: Report of Examination (Data Extraction), Report of Examination, and Discontinuation Report.

7.4.1. Report of Examination (Data Extraction)

7.4.2. This report is used when only the data extracted from an evidence item(s) is provided to the requester. No forensic interpretation/analysis has been conducted and no forensic opinion is offered.

7.4.3. Using the DEUF04 – Report of Examination (Data Extraction) template, fill out the sections to include scope, evidence items, tools/methodology, extracted data details, disposition and signature of analyst.

7.4.4. Copy the extracted data to media to be passed to the requestor. Files and folders can be compressed in an appropriate container (i.e. ZIP) if the data would best be transported in a compressed file.

7.4.5. In LIMS mark the items as "Draft Complete" for technical and administrative reviews to be completed.

7.4.6. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

7.5.   Report of Examination

7.6.   This report is used when forensic interpretation and analysis of the evidence item(s) has been conducted, whether a forensic opinion has been offered or not.

7.6.1. Using DEUF07-Report of Examination template, fill out the sections to include the scope of examination, tools/versions used, methodology (e.g., recover folders, hash/signature analysis, etc.), the results and the conclusion / finding of the report. These items are recorded on DEUF05-Forensic Examination for inclusion into the Report of Examination.

7.6.2. If applicable, use DEUF11 – Digital Evidence Report template to create a report. This report template is used in addition to the Report of Examination when the analysis requires an opinion from the analyst, interpretation of finding or more extensive reporting is requested or determined than on the Report of Examination.

7.6.3. Once complete, mark "Draft Complete" in LIMS for technical and administrative reviews.

7.6.4. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

7.6.5. Discontinuation Report

This report is used when analysis/extraction requested cannot be completed, the requestor has cancelled the request or the request/data/evidence is no longer available to the digital evidence unit.

7.6.6. Using DEUF08-Discontinuation Report template, fill out the sections as appropriate.

7.6.7. Once complete, mark "Draft Complete" in LIMS for technical and administrative reviews.

7.6.8. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

8. Sampling

8.1. Not applicable

9. Calculations

9.1. Not applicable

10. Uncertainty of Measurement

10.1. Not applicable

11. Limitations

11.1. The scope of the report will be limited to the scope of the request for examination.

12. Documentation

12.1. DEUF05 DEU Forensic Examination Form

12.2. DEUF04 DEU Report of Examination (Data Extraction)

12.3. DEUF07 DEU Report of Examination

12.4. DEUF11 DEU Digital Forensics Report template

12.5. DEUF08 Discontinuation Report

13. References

13.1. Forensic Science Laboratory Quality Assurance Manual, (Current Version).

13.2. FSL Departmental Operations Manuals, (Current Versions).

13.3. FSL Laboratory Operations Manuals, (Current Versions).

13.4. Digital Evidence Unit Quality Assurance Manual (Current Versions).